

SYSTEM AND METHOD FOR SINGLE SIGN ON PROCESS FOR
WEBSITES WITH MULTIPLE APPLICATIONS AND SERVICES

INSAI

FIELD OF THE INVENTION

The present invention generally relates to systems and methods
5 for providing access to financial accounts and more particularly to systems and
methods for sign up, log on and ownership verification procedures for
providing access to a plurality of financial accounts over the Internet.

BACKGROUND OF THE INVENTION

As with most industries, the Internet has significantly affected
10 the way in which the financial industry communicates with its customers.
Most significantly, major financial institutions have found providing their
customers with online access to their accounts both desirable, cost effective,
and indeed necessary to remain competitive.

The financial industry faces special hurdles in providing online
15 access to customer's accounts due to the very nature of the accounts being
accessed. The account information maintained by financial institutions is
probably the most important and private personal information that an
institution can hold for a person. Accordingly, controlling access to this
information is one of the most significant duties that must be performed by a
20 financial institution.

Most large financial institutions have various divisions that
separately handle different types of accounts for their customers. For example

one division maintains personal banking accounts (e.g., checking and savings), another division handles mortgages, while yet other divisions are responsible for maintaining credit card and investments respectively. Furthermore, each of the types of accounts is typically governed by a different set of regulations.

5 For example, the rules that govern a checking account are completely different from the rules that govern an investment account. For these reasons as well as others, the divisions within a financial institution have traditionally operated independently, each developing their own systems and methods for operating their particular line of business. Unfortunately, the development of these

10 separate systems has included the separate development of Internet interfaces for communicating with customers. These separate interfaces are confusing to the customer and do not provide a uniform appearance of the financial institution to its customers.

Some financial institutions have attempted to solve this problem
15 by provided links on a single institution web page that lead to the various systems of the divisions of the institution. One significant problem that persists is that a customer must separately sign up, verify ownership, and log onto the separate systems, providing separate passwords and separate verifications of ownership.

Other institutions have solved this problem by requiring
20 ownership of a specific type of account (e.g., a checking account) and manually linking or otherwise associating the privileges of access of all other types of accounts to the required account. This reduces the number of customers with access to their account information and transaction capability
25 to the customer base of the required account.

It is therefore an object of the present invention to solve the problems of the prior art in a system and method that requires only a single

sign up, verification and single ID for a website that includes multiple applications and multiple services.

SUMMARY OF THE INVENTION

The system and method of the present invention integrate the Internet front-end log on processes of all of the various systems of the institution. In this manner, the present invention provides a singular way for a customer to identify that they are a customer of the institution, regardless of the application or services that the customer ends up using on the Internet website of the institution. In a preferred embodiment, the single sign on processes are used for customers of a financial institution to view and conduct transactions with respect to their accounts with the institution. These accounts include but are not limited to checking and savings accounts, mortgages, credit card accounts, investment accounts, online trading, auto loans and leases, home equity loans, personal loans, trust accounts, 401k accounts and insurance accounts.

During the initial sign up for the online access to its accounts, a customer creates their User ID and password online during the same session. There is no need for the institution to mail the User ID or password to the customer. This same sign up process allows the customer to provide verification of ownership to obtain rights to information and services available online for their accounts. Once the customer has logged on (password) and verified their ownership of at least one account, the system displays all of the customer's accounts that are available for access via the Internet website. In addition to signing up existing customers, the present invention permits the creation of non-authenticated IDs for potential customers to use (or for customers to use for non-account access). For example, a non-customer can

be provided access to online account opening services, pre-populating application data with their account information saving account application data, viewing status of new account application, and saving calculator and financial planning data.

5 A significant feature of the present invention is the online verification of ownership by a customer. Based on identifying information entered for one account, the list of all accounts owned by the customer is presented to the customer to choose which accounts they want to access online. Online ownership verification uses only a single account of the customer and the verification criteria associated with the account. A customer may have several accounts with the institution, but may only choose to view only one or two online (although the customer may choose to view all the accounts). From the selected accounts, the system of the present invention creates an verification hierarchy with respect to the accounts. The hierarchy places the selected account in the order of difficulty of the verification. When determining the verification questions to use for the single account, the present invention selects the account from the hierarchy with the most stringent requirements. The verification of ownership required for the different accounts might be less or more stringent based on the risk of the account and the lack of accessibility of verification data to the general public. For example, the verification required for access to credit card or deposit accounts is the most stringent, requiring a code only available on the back of the card or a PIN known only to the customer. Once the account that is highest in the hierach is verified, all other account that are equal or lower in the hierarchy are considered verified as well.

10

15

20

25

Once a customer has signed up and logged on, the present invention displays all customer accounts that the customer has selected for

viewing (including account balances) on an account summary page. This account summary page allows the customer to then navigate to the line of business site to see more details or transact using the account. Once signed up for the online process, customers are able to add additional accounts online once they are available online or once a customer acquires a product. This process may not require additional verification of ownership, depending on where the new product falls in the verification hierarchy.

Sub 17

In subsequent logons to the system, the present invention allows customers to re-identify themselves to see a forgotten ID, and to re-verify themselves so they can recreate a password if a password is forgotten. The present invention allows the customer to create answers to challenge questions that only the user should know the answer to. For example, a challenge question could be, "what model was your first car?". The answers to the challenge questions are stored in the system for future use if the user forgets his password. If the situation occurs that the user does forget his password, he is presented with the challenge questions to which he previously provided the answers. If the user successfully answers the challenge questions, he is allowed access to the system (and is allowed to change his password).

In addition to the challenge questions, the user is also able to create "cue" questions. The cue questions provide the user with a hint as to the user's selected password. For example, if the user selects the name of his dog as his password, the customer can create a cue question such as "What is your dog's name." If the user forgets his password, he is first presented with the cue question to see if the user can recollect the password. If the cue question does not jog the user's memory, he is then presented with the challenge questions that allow the user to re-identify himself to the system.

5

10

15

20

25

Sub B2

The present invention is not limited to providing access to personal accounts and is equally applicable to business accounts. Business customers can use the system for online enrollment, fulfillment and ownership verification. This includes customers who want to see both personal and business accounts under one ID and password. The business owner may be a sole proprietor (using a social security number), a business owner or partner (using a tax identification number (TIN)), or a multiple business owner (multiple TINs). Furthermore, the system allows a tiered authority structure where an owner of an account can set up and authorize access to the same or lesser levels of authority to non-owners of the accounts (e.g., spouses or employees). This allows set up and monitoring of sub-IDS for consumers as well as businesses.

Another significant feature of the present invention is its ability to allow the customer to self-service their sign up, logon, and forgotten ID or password processes without having to contact customer service or wait for information to be given or sent to them.

Sub B3

The present invention provides ease of use by the customer since the customer does not need to duplicate work such as inputting his or her social security number, account number, and other personal or account information a number of different times to either sign up for access or to logon to see their accounts. The ability for the customer to use "self-service" sign up and logon failure procedures eliminates or minimizes customer and back office support for fulfillment (e.g., issuing IDs, passwords, and reissued passwords). The single sign on ID and password that allows access to all of the customer's accounts provides speed of fulfillment, ease of use and reduced customer support for issued or forgotten IDs and passwords. The ability for customers to see all of their accounts with one logon eases the customer experience and

Sub B3

enhance customer retention, as well as enhancing cross-sell and up-sell efforts.

BRIEF DESCRIPTION OF THE DRAWINGS

For the purposes of illustrating the present invention, there is shown in the drawings a form which is presently preferred, it being understood however, that the invention is not limited to the precise form shown by the drawing in which:

Figure 1 illustrates the hardware of the system of the present invention;

Figure 2 depicts an overview of the sign up and log on processes of the present invention;

Figure 3 shows a detailed flow of the sign up process; and

Figure 4 illustrates the authentication process.

DETAILED DESCRIPTION OF THE INVENTION

Referring now to the drawing figures in which like reference numbers refer to like elements, there is shown in Figure 1 a diagram of the hardware elements of the system of the present invention, designated generally as "100".

Sub B4

System 100 illustrates the system of the present invention that allows customers 110 to use a single sign on procedure to obtain access to a plurality of their accounts residing on the systems 192-196 for different lines of business in the institution. Customers 110 use their workstations 110 to connect to system 100 through a communication network 115. In a preferred embodiment, the network 115 is the public Internet, but can be any other communication connection such as a direct dial up line or a third party value

Subpt 7

5

added network. Customer workstations 100 are comprised of any platform capable of running an Internet web browser or similar graphical user interface software. Examples of suitable web browsers include Microsoft's Internet Explorer™ and Netscape's Communicator™. The platform for user workstations 100 can vary depending on the needs of its particular user and includes a desktop, laptop or handheld personal computer, personal digital assistant, web enabled cellular phone, web enabled television, or even a workstation coupled to a mainframe computer.

Subpt 7

15

20

25

In the preferred embodiment, customer workstations 110 communicate with system 100 using the Transmission Control Protocol/Internet Protocol (TCP/IP) upon which particular subsets of that protocol can be used to facilitate communications. Examples include the Hypertext Transfer Protocol (HTTP), data carrying Hypertext Mark-Up Language (HTML) web pages, Java and Active-X applets and File Transfer Protocol (FTP). Data connections between customer workstations 110 and data communication network 115 can be any known arrangement for accessing a data communication network, such as dial-up Serial Line Interface Protocol/Point-to-Point Protocol (SLIP/PPP), Integrated Services Digital Network (ISDN), dedicated leased-line service, broadband (cable) access, Digital Subscriber Line (DSL), Asynchronous Transfer Mode (ATM), Frame Relay or other known access technique. Web servers 120 are coupled to data communication network 115 in a similar fashion. However, it is preferred that the link between the web servers 120 and data communication network 115 be arranged such that access to web servers 120 is always available.

It should be noted that although customer workstations 110 and

web servers 120 are shown as each coupled to a single data communication network 115, this arrangement is shown merely for the convenience of aiding

explanation of the present invention and is not limited to such. For example, data communication network 115 can be the Internet or other public or private network comprised of multiple communication networks, coupled together by network switches or other communication elements. Between the
5 communication network 115 and the web servers 120 of system 100 is a "soft" firewall 117. Soft firewall 117 is firewall that is erected using only software techniques (as opposed to firewall described below).

Web servers 120 are comprised of one or more central processing units coupled to one or more databases (not shown). In addition,
10 web servers 120 further comprise a network interface (not shown) to couple the processor to data communication network 115, and include provisions for a web site or other technology which can create a network presence from which the provider of web servers 120 can interact with customer workstations 110. Technologies including hardware and software for establishing web sites such
15 as an Internet web site are known.

Web servers 120 can be comprised of any suitable processor arrangement designed to accommodate the expected number of users and transactions for the particular system in which these elements will be implemented (hence the illustration of three web servers 120 in Fig. 1).

Known software languages and database technologies can be used to implement the described processes. The databases and programmatic code used by web servers 120 are stored in suitable storage devices within, or
20 which have access to, web servers 120. The nature of the invention is such that one skilled in the art of writing computer executable code (software), would be able to implement the described functions using one or more popular
25 computer programming languages such as "C++", Visual Basic, Java or HTML.

The web servers 120 are each coupled, through a separate firewall 125, to application server 130. The firewall 125 is comprised of both hardware and software components as well known in the art. Firewall 125 is required to protect the confidential information contained in system 100
5 illustrated below firewall 125 in Fig. 1. As implied by its title, the application server 130 is where the applications employed by the web servers 120 reside. Coupled to the application server 130 is a database 135. Aside from other data, the customer profiles containing the user IDs, passwords and relationship and profile data is stored. Although not shown, database 135 can include a
10 suitable database management system processor which operates thereon. In addition, although database 135 is shown as a separate entity in Figure 1, it is contemplated that database 135 can be implemented as part of a storage device within the application server 130, or can even be coupled to application server 130 across a communication link. Database 135 is preferably a
15 multidimensional database that is analyzed using on-line analytical processing (OLAP) tools.

The application server 130 is coupled to the systems of the various lines of business 190-196 through a communication server 140 and a delivery processor 145. As described below, if a customer wishes to view more detailed information regarding an account, or wishes to conduct some transactions, the user is coupled to the specific line of business system 190-
20 196 that maintains the desired account. The communication server 140 and the delivery processor 145 together they serve as a middleware component for communication between the application server 130 and the line of business systems 190-196.
25

Sub B67
Figure 2 illustrates an overview of the sign up and log on processes of the present invention. In step 200 a customer is presented with an

Step 107

5 up-front filter asking them to define themselves as a business, personal, both business and personal, or if they are not a customer. Prior to the customer continuing in the process, a warning is presented to the customer with respect to the dual signature limitation for business customers. Based on the self-selection, the customer is presented with an explanation in regard to the linking personal and business accounts, the single signer requirement, and the necessity of signing up business accounts first.

10 For business customers, system 100 collects business name, individual name, email, TIN, one account number and type. Then, system
100 identifies that the business customer exists based on a Customer Identification File (CIF) contained in database 135 (see Fig. 1) by matching on TIN and account number.

15 For personal customers, system 100 collects first and last name, e-mail address, social security number, and account number and type. System 100 then uses the social security number and account number to identify that they exist.

20 In step 205 the customer selects his own User ID and Password. The User ID is preferably 8-20 characters in length, while the password is preferably 6-10 characters in length with one alphanumeric and one numeric character. The password is also preferably case insensitive. This ID and password is created whether or not the customer was successfully identified in the previous step. If the customer was successfully identified, they will be allowed to continue the sign up process. If system 100 was unable to identify the customer, the customer is requested to call customer service to identify the problem and to continue the sign up process via the call center. Because the customer has already selected their ID and password, the call center representative is able to easily identify the customer using the ID and the

customer does not have to wait for fulfillment of an ID and password in the mail and is able to logon to the system after completing the call with the customer service representative.

Sub 87 5 After creating the User ID and password, the customer is presented with the option to select challenge questions, which as described below, enables them to reset their passwords online, by themselves, in the event the customer forgets the password selected. In step 210, the customer is then presented with an online legal agreement that must accepted prior to the customer continuing. The online legal agreement contains all of the terms and conditions of the customer's use of system 100. For those customers who were set up via the call center, this legal agreement is presented to them upon logging on for the first time.

Sub 87 10 In step 215, the customer is shown all of his/her accounts (including business accounts if applicable) that he/she has with the institution. The account information is presented to the customer based on data contained in the customer's CIF profile. After the accounts have been presented to the customer, the customer is given the option to view these accounts using system 100. In addition to the accounts the customer can view, the customer is shown all services (e.g., tax, payroll, wire transfer, and electronic billing services) in which the customer able to participate.

15 20 25 In step 235, the customer is presented with a set of verification of ownership questions based on the accounts the customer has selected to access. As previously described, the ownership verification procedure follows a hierarchy where the customer is asked questions based on the "highest level" product he has selected to access. In a preferred embodiment, for personal customers, credit card accounts are the highest level, followed by deposit, loans, investments, and mortgages. All products are represented and have an

assigned level within the verification hierarchy. If the customer passes verification, he/she has completed the sign up process, is presented with a screen confirming which accounts they can access and can proceed to logon to access their accounts. If the customer fails verification – for example, due to missing information on the host systems – the customer can “drop down” to the next account type on the hierarchy or contact Customer Service for assistance. Upon successfully passing the lower level verification questions, the customer will have rights to access those accounts and any accounts lower in the hierarchy, but will not have the rights to access the accounts that were represented by the failed, higher level of verification questions.

In the initial sign-up process and during subsequent log ons, system 100 checks to ensure the customer has a browser that provides adequate security measures (e.g., encryption). This check also validated that the customer can receive cookies and has javascript enabled on their browser settings. This security is required because of the sensitive financial nature of the information being provided to the customer. In a preferred embodiment, the customer’s browser supports 128-bit encryption. When the user clicks on ‘Sign Up’ or ‘Log On’ from the main welcoming screen of system 100, or when the user attempts to access a protected resource, the browser check is completed. If the user’s browser is detected with less-than-128-bit encryption the user is given the option to download the latest browser/patch or given instructions on how to correct his situation. In addition, a self-check function is provided for customers when learning about system requirements for signing up.

Figure 3 illustrates the detail of the sign up process. The sign up procedures allow a new user to create an online User ID and Password. In addition, if this user is also a customer of the financial institution, he/she can

register for access to his accounts. As previously described, the present invention operates, in a Graphical User Interface (GUI) environment, in which the users are presented with a series of screens. The screens allow the system 100 to both elicit information from the user (e.g., selections) and present 5 information to the user (e.g., account summaries). In the sign-up process, the first screen presented to the user is filter screen that asks the customer which accounts he would like to access (see step 300). In a preferred embodiment, the choices on this filter screen include: Personal Only, Small Business Only, Both Personal and Small Business using one User ID, Both Personal and 10 Small Business using two User ID's, and "I do not have accounts with the institution". Depending on the selection, the user is presented with a brief description of the Sign Up process and features and benefits information. The filter pages are used to determine whether the user is presented with the Personal, Small Business, or Prospect Identification questions.

15 In step 305, the user identifies himself or herself to system 100. Depending on the entry point, the identification process differs slightly. A user coming for account access is asked if they are trying to access their personal, small business, or both accounts. If they select personal, they will see a personal identification screen. If they pick either Small Business or 20 Both, they will start at the Small Business identification screen.

Sub B397
Each of the identification screens prompt user for information sufficient to retrieve the customer's information from the CIF. This information includes the Social Security Number (SSN) for access to personal accounts, the Taxpayer Identification Number (TIN) for access to business accounts, the customer's account number and account type, the user's first and last name and email address. The email address portion of the input screen for identification also has a check box to allow users to opt-in for marketing email 25

messages.

5

Additionally, customers are requested to choose a country from a drop-down with a list of countries. The entry for the United States is the default and other countries are preferably listed alphabetically. If the user chooses United States, he is also prompted to enter a zip code. This information is collected to understand which regulatory requirements a customer may be covered if they choose to apply for a product line.

10

The account type field is populated from a selection by the user from a drop-down list box of account types. The presentation of this drop-down list varies depending on the type of user. Users coming through an access point other than signing up for account access are presented with a complete list of all account types that are on CIF. In a preferred embodiment, the following are the types of accounts accessible from system 100: Credit Card; Mortgage; Checking; Savings; Overdraft Line of Credit; Credit-on-Demand; Certificates of Deposit (CDs); Money Market Account (MMA); IRA – CD; IRA – Savings; IRA – MMA; Investments; Personal Loans; Auto Loans; Home Equity loans and Line of Credit; and Insurance.

15

20

25

The user iterates through the identification screen until all mandatory fields are entered in the proper format. Next, the social security or TIN and the account number are used to query the CIF for a match. If a CIF# record is found for this user, system 100 checks to see if a user ID associated with this CIF# already exists in the system 100. If such a user ID is already associated with the CIF for the customer, system 100 displays the ID to the user and explains that multiple ID's are not allowed. In this case, the user is given the option to Log On with this ID (see below) and explain to him that if he was trying to "add" or "show" an account, he should Log On and use the Show/Hide Accounts link to accomplish this. If the customer never finished

the Sign Up process previously begun, the customer is provided a link to Log On and the customer is presented with the screen applicable to their next step in the process. System 100 also asks the user if he has forgotten his password and provides a link that takes the user to Log On/Re-authenticate flow (see 5 below).

The process varies slightly for prospects (users with no accounts with the financial institution). For a prospect, the user is prompted for First 10 and Last Name, Email address (required), Company Name, and an indicator of their interest (personal products, small business products, or both). This user is automatically passed to the Create ID/Password, step 310, since there is no need to perform a CIF match.

Sub 310 In step 310, the user is prompted to Create a user ID, a password and challenge questions. Regardless of whether the user is identified on the CIF, the user is allowed to create an ID and password that are added to the 15 database of system 100. Prospects (users without current accounts) are allowed to establish a user ID and password in order to facilitate Sign Up at a later time or to access non-account features, such as saving data to a calculator or application or personalizing a financial utility page. The user is created in the system by adding the ID, password and email address to the database. If 20 the user has been identified as a customer with current accounts, the customer's CIF number is also stored in the database with the ID and password..

Sub 311 At this point in the sign up process, the user is also prompted to select and answer challenge questions. These challenge questions replace the prior art method of re-verifying using account information. The user selects 25 one question from each of three drop down list and completes the answers. Users that have passed the CIF match (i.e. customers) have the option to opt-

Sub B11 out of challenges. If they choose to do so, they will not be able to re-verify online and create a new password. They would have go through the customer service center of the institution and a new password is mailed to them. As previously described, the challenge questions are personal in nature, of a type that only the user would be able to answer them (e.g., what was your first grade teacher's name).

After the user completes the user ID, password and challenge question fields, the customer is presented with a verification screen where she has the opportunity to go back and change the user ID, password, and/or challenges if they are not correct. If the user is not found on the CIF and the user attempted a CIF match, he will be assigned a role indicating he has not been identified as a customer of the institution (denoted as an UNAUTH user). The treatment of these users is the same as prospects. The Sign Up process ends at this point for users not found on the CIF. They are presented with a dynamic customer support screen.

Sub B12 In step 315, the user is presented with the legal agreement governing the user's access to system 100. All users creating a user ID and password have to accept the legal agreement. This is equally true for prospects and customers that have both passed or failed the CIF match. Since these users will have other functionality at the site, they all need to accept the legal agreement. The user is presented with the legal agreement and has the option to "I Agree" or "I Disagree" or "Print". If the user rejects the disclosure, she is notified that she cannot continue with the sign up process and is presented with the option to view it again. If the user accepts the disclosure, the sign up process continues.

Sub B13 After the user accepts the legal agreement, there is a decision point before proceeding to the next step. If the customer was coming from a

Sub B13

process other than signing up for account access, the user will be prompted to Log On (see below). After successfully logging on, the user is returned to the process that brought him to Sign Up. If the user is signing up for account access, the user will continue with show/hide functionality.

5 As part of the sign up process, the user is prompted in step 320 to select accounts the she would like to access using system 100. The user is presented a list of her accounts/relationships with the institution and is prompted to select “products” she wishes to web-enable. The list of relationships is presented to user in the form of a checkbox list with product names, and partial account numbers. After selecting accounts to activate, the user is presented any associated legal agreements and further authentication further verification of ownership questions, based on the products/services he has chosen and the placement of the products in the verification hierarchy. The authentication process is described in more detail below.

10 In addition to providing access to accounts, the customer is also able to access services that are associated with the selected accounts. For example, a wire transfer capability is presented if the customer has selected a DDA (checking) account. The reason that these services are presented separately is that they may 1) be available only to certain products and 2) may have fees associated with their selection or 3) may have a special legal agreement or registration process associated with it. As a result, the customer cannot be given automatic rights to the service.

15 The final step in the sign up process is the log on step 330. After the user completes the activate accounts process of step 320, the user receives a welcome and confirmation screen and is prompted to log on to access their accounts. At the same time, a request to generate and mail an Enrollment Verification Letter (EVL) to the user’s home address on record is sent to the

back office of the institution. This letter provides an out-of-band notification that the user has been enabled to access and transact on their accounts online and is used to discover fraud attempts if someone other than the customer has obtained knowledge of the identification and verification of ownership data.

5 The user receives this EVL once, i.e. the very first time he signs up (not during subsequent enabling of accounts). In addition to the letter, the customer is sent a real-time email (if an email address was provided in step 305), which will confirm his enrollment.

10 Figure 4 depicts in more detail the ownership verification process. In order to enable access to view or transact against accounts, a customer must undergo an ownership verification as is illustrated in Fig. 4. This ownership verification process is used by both new and registered users to verify ownership of an account whenever a customer attempts to “show” accounts that require a higher level of verification than what she currently has.

15 As previously described, verification for online access is based on a hierarchy of products within the institution. Customers who verify ownership (correctly answer questions for a particular product) are verified authenticated for each of the products below it in the hierarchy. For example, individuals who enable their checking and mortgage accounts for online access are verified with questions based on their Checking account, since checking is at a higher level in the preferred product verification hierarchy defined by the institution. If the same customer later decides to enable their credit card account online, they must answer additional questions, since the credit card account is higher in the hierarchy than the customer’s current level of verification. By the same token, if the customer later chooses to enable his auto loan account , he is not required to answer any further verification questions since his current level of verification supercedes that required by

auto loans.

Sub B14

Verification according to the present invention is different from the prior art authentication for several reasons. First, some of the prior art verification questions are not applicable to the Internet channel or to the "self-service" methods of the present invention. For example, a question related to a "a recent transaction" cannot be prompted and verified by a system such as system 100 in real time. The verification questions of the present invention relate to access to accounts via the Internet Channel, and are not related a global name or address change.

Prior to entering the verification process of the present invention, the user must have accepted the acknowledgment(s) and or agreement(s) for all product types for which the system is attempting to verify the customer for (see step 315). Once ownership is verified, the verification level and date is updated on user profile in the database of the system 100. If the user was directed to the verification screen because she was requesting access to a new account, the user is returned to the select accounts screen (see step 320 in Fig. 3).

Sub B15

Of the products the customer has chosen to activate online during the select account process (step 320 of Fig. 3), an account of the "highest" product type on the hierarchy is be chosen to verify against. If multiple accounts of this product type have been selected, the system performs the following logic to determine which account to use for product-level verification. If the product type for verification is the same type that the user identified himself with during sign up/identification, the account number chosen during identification is used. If the product type was not used for identification, then the first account returned on the list is used.

Sub B16

In step 400 it is determined if the authentication level for the

Subfile 7

current product/account selected is greater than the current level of verification performed by the user. If it is not, the process proceeds to step 425 in which the user is confirmed for the present level of verification. In a preferred embodiment of the present invention the hierarchy implemented for personal customers opposed to business customers) is: Credit Card; Checking/MMA (excluding IRA MMA); Savings/IRA MMA/IRA Savings; CD/IRA CD; Overdraft Line of Credit; Investments; and Mortgage. The customer's SSN is not used for verification of a product since the user has already entered it during the Sign Up/ Identification process. If a higher level of verification is required, the system in step 405 checks to see if there is a complete record for the account in the database of system 100. If there is not a complete record, an error message is generated in step 407

In step 410, the user is presented with a list of fields and asked to enter verification of ownership information based on the specific account selected from the hierarchy. All verification fields presented to the user are required to be filled out. The user iterates through the screen of verification questions until all fields are entered. (Note that this data is validated only for completion at this point and is not yet compared to the database). System 100 notifies the user as to which required fields are missing, if any. System 100 refers to the product section for the verification questions to be asked for each product. In step 415, system 100 verifies that all of the fields have valid data. If there is invalid data (e.g., a missing digit in an account number) an error message is generated in step 417 and the user has the chance to fix the data.

Once all mandatory fields are entered, the user has three attempts to modify the verification information before the verification of ownership process is halted (step 420). For security reasons, when information is incorrect, the specific field will not be highlighted. A generic

message is used, such as "Verification failed. Please try again." Once the user has successfully verified, the verification is confirmed in step 425 and the user is able to then log on (step 430). The user's profile is updated with the "new" verification level and date and a log transaction is created.

5 If the user is not able to present accurate information for authentication after three tries in step 420, it is determined whether the user has provided enough information for authentication for at least one product/account. If she has, the confirmation of step 425 is followed. If there is insufficient authentication for any product an error message is displayed in step 435 and the authentication processes is exited in step 440.

10 *Subj17* The following are some examples of the verification questions required for access to specific accounts. For credit card products, it is required that the user enter the trailing 4 digits for all of the accounts they are selecting to "show". If the user incorrectly enters the trailing digits for the account being used for verification, then, after three attempts, the user fails verification altogether. However, if the user incorrectly enter the trailing 4 digits for an account not being used for verification, then the user just does not have online access to that account. In addition to the account number, the user will prompted to answer questions related to the following: Mother's Maiden Name; the CVV/C2 number printed on the reverse side of the physical credit card; Date of Birth; and Home Phone Number.

15 If the user's highest account in the product hierarchy is the checking equivalent product account or if the user has a credit card with incomplete information and he has a checking account, the following information is required for verification. Checking equivalent accounts include accounts such as a Money Market Account (MMA). The verification information required for access to a checking account includes: Account

number; Mother's Maiden Name; Transaction Amount (e.g., exact amount of last withdrawal); Posting Date (of last transaction); Last Deposit Amount; and Last Deposit Date.

- If the user's highest account in the product hierarchy is the
- 5 checking equivalent product account or if the user has a credit card with incomplete information, he does not have a checking account and he has a savings account, the following information is required for verification. Savings equivalent accounts include a complete savings family of Savings, IRA MMA, and IRA Savings accounts. The verification information required for access to a savings account includes: Account number; Mother's Maiden
- 10 Name; Last Deposit Amount; Last Deposit Date; Transaction Amount (e.g., Withdrawal); and Posting Date.

- If the user's highest account in the product hierarchy is the Certificate of Deposit (CD) equivalent product account or if the user has a credit card with incomplete information, he does not have a checking or savings account and he has a CD account, the following information is required for verification. CD equivalent accounts refers to a complete CD family of CDs and IRA CDs. The verification information required for access to a CD account includes: Account number; Mother's Maiden Name; Date Opened; Original Principal Amount; Maturity Date; and Posted Interest.
- 15
- 20

- If the user's highest account in the product hierarchy is an investment account. Auto loan, personal installment loan, home equity loan, or mortgage, and the customer identified themselves in step 305 with that account, the customer is not presented with verification questions in the preferred embodiment since the business requirement is that the customer verify themselves using only a social security number and an account number. If they did not identify themselves in step 305 with the highest account in the
- 25

verification hierarchy, the customer is requested to complete the account number of the account which is at the highest level.

Sub B18

5 The verification of ownership processes for online access for Small Business customers is dependent on whether or not the customer has a deposit product in their profile. As with personal authentication, if a business customer verifies or correctly answer questions for a particular product, they are automatically verified for each of the products below it in the hierarchy. Verification requirements for Small Business customers differs from that for Personal customers. Products available for online access are Checking, MMA, 10 Savings, CD, Credit Card, Revolving credit products and Investments. As a rule, a business customer must either verify ownership against a deposit account or an investment account. In a preferred embodiment, small business customers will not be able to verify against any other accounts. In the preferred embodiment, the verification hierarchy for small businesses is as 15 follows: Checking/MMA; Savings; CD; and Investments.

As a result of the aforementioned rules, a business customer in the preferred embodiment will only be able to verify ownership against their Deposit or Investment accounts for online access. Once verified, the customer can access all the products below the deposit account in the hierarchy.

Sub B19

20 Although described briefly before, the follow generally describes the log on process. When a user logs on, several scenarios exist based on varying ID and password combinations in put by the user such as valid ID/invalid password, invalid ID/invalid password, etc. Although each of these scenarios are a bit different, it has been learned that if the scenarios are treated differently, the system 100 will reveal information regarding a "hit" on a valid ID, as well as information regarding the security and authentication logic and User ID status within the system. To ensure that system 100 does not leak any

Sub B19

such information, all scenarios with regard to invalid ID/PW combinations are treated identical. The customer has the ability to click on a "Having Trouble?" link and be presented with Help options (that is, contact customer support or re-authenticate online options).

5 If the user types in a valid ID/valid Password combination, the system 100 logs the user in successfully. If the user types in a valid ID but has used the same ID for three consecutive log on attempts (not necessarily in the same session) and this is a valid ID, system 100 locks the user out. A User ID is locked after three (3) unsuccessful log on attempts with invalid
10 passwords over an infinite number of days without a successful log on. A counter within system 100 tracks the number of unsuccessful log ons. This counter is reset upon successful log on. Once a User ID is locked, it will remain locked indefinitely until the user re-authenticates online or calls Customer Support. (Customer Support has a function to unlock IDs) Even
15 though a User ID is "locked", the user will not see any change to the logon screen. The same logon screen will continue to appear regardless of the number of failures. The user is not told that the User ID has been locked. There is a link titled "Having Trouble?", which when clicked, instructs the user to contact Customer Support or Re-authenticate online.

20 If the user types in an invalid ID and an invalid password, system 100 provides a global parameter to detect this situation by sending an alert message to a pre-defined list of administrators when there have been, for example, 1000 failed log on attempts in 5 minutes. Due to the security risk of information leakage if a different screen is presented, this user will not see any change to the log on screen, but will see the same "Having Trouble?" link.

25 As seen above, in the simplest case, the user logs on successfully and goes to the Account Summary page to view their accounts. However,

there are several other situations that must be accounted for, such as a user exceeding the maximum number of consecutive log on attempts (using the same ID), the user has forgotten his password, or the user has received a pre-expired password in the mail and is attempting to log on.

5 If the user forgets his password or his ID, he can re-authenticate himself to the system using the procedures described above with respect to challenge questions. An additional feature of the present invention is the use of "cue" questions. As part of the initial sign on process, or at a later time, the user is able to cue questions that provide the user with a hint as to the user's selected password. For example, if the user selects the name of his dog as his password, the customer can create a cue question such as "What is your dog's name." If the user forgets his password, he is first presented with the cue question to see if the user can recollect the password. If the cue question does not jog the user's memory, he is then presented with the above described challenge questions that allow the user to re-identify himself to the system.

10

15

After a user has successfully logged on, the user's profile is scanned for any accounts for which the user has not accepted associated legal agreements. In addition, if a legal agreement has been updated and Legal determines that all users must be re-disclosed, such disclosures are presented to the user again for acceptance. Access is not granted to a product type until all required legal agreements have been accepted.

20

The log on function also takes into account the fact that a user will not automatically be going to the Account Summary page. Prospects (non-customers) sign up to system 100 to utilize a function other than seeing account information. When a Prospect or a customer coming from another process than account access completes the sign up process, she is directed to Log On. Upon a successful Log On, this user is then returned to the proper

25

process. For example, if a user is coming from another process, the user is returned to this process instead of being taken to the Account Summary page. For example, a user might be following a URL to see the status of an online application for a mortgage account. This page is protected, thus requiring the user to Log On before being presented with the page that contains the customer's personal information. Upon a successful logon, the user should be brought directly to the page she requested.

The log on process also presents the opportunity to collect challenge questions from current customers if they have not already done so. Upon a successful logon, the user is prompted to select and answer challenge questions. As previously described, these questions replace the verification of ownership using account information. The user selects one question from each of three drop down list and completes the answers. Since these are all customers of the institution, they will have the option to opt-out of challenges. If they choose to do so, they will not be able to re-authenticate online and create a new password. They would have go through the help center and a new password is mailed to them.

One of the significant features of the present invention is the ability for a customer to re-authenticate himself or herself to system 100, such as in the case of a forgotten password or user ID. Typically a user is directed to the re-authentication page from the log on screen, when the user has unsuccessfully tried to log on. Successful re-authentication allows the user to subsequently change his password. The "new" password is not validated against the "old" password to verify that they are different – thus, a user who has hit the maximum failed log on attempts can "reset" his password to the same password. At this point, the user is taken back to the Log On page.

For re-authentication, users will be presented with two of the

three "challenge" questions that were originally created during sign up or log on as previously described. The user answers to these questions during re-authentication must match the answers they previously provided. In a preferred embodiment, if the user unsuccessfully attempted to re-authenticate online 9 number of times in the last 30 days, the user will not have the ability 5 to change their password online. These users are stopped before challenge questions are presented and given an error message instructing them to call customer service. For example, the user can only try and re-authenticate during 3 sessions in 30 days.

If a user is eligible to re-authenticate online using challenge 10 questions, system 100 randomly selects two of the three challenge questions and presents them to the user. The user has three opportunities to answer these questions. If they do not pass after three attempts, the user is directed to an error screen. If the user successfully answers these questions, they are then 15 able to change their password online.

As previously described in relation for Fig. 1, the purpose of the sign-up, log on and verification procedures is to allow customers to view all of their accounts with the institution though a single interface with a single sign on process. The account summary page of the present invention summarizes 20 all of the accounts in a balance sheet format that the customer has selected to "show" and for which the customer has been verified. Each account that the user has selected to "show" for online access is displayed on this screen under either the "Deposit", "Credit Card and Revolving Credit", or "Mortgage and Loans" main heading . When the user clicks on a specific account to view 25 details, he enters the system for the specific line of business (LOB) (see 190-196 in Fig. 1).

On the account summary screen, the user is presented with a list

of their enabled accounts, from which they can make a selection to see more details. They make their selection by clicking on the relevant hyperlinks, which brings the user into the appropriate LOB site supporting the selected product/account. For example, the supporting LOB site could be online banking, mortgage servicing, investment or trading or credit card servicing.

5 This screen also contains summary (balance) information for each of the accounts presented to the customer. This information will vary depending on the type of account.

When the user comes to the account summary screen, system
10 100 uses the customer profile to determine which accounts to display on the summary screen. The user's accounts are validated with the respective LOB system once per session. The validation consists of verifying that the account still exists and that this status is still valid. In the case of an invalid status or account that no longer exists, a pop-up window instructs the user that account
15 has been removed from his online portfolio and provide the phone number for customer service. The account title and account number (with certain digits masked) are displayed for all enabled accounts. The account summary
masking (balance) information for each of the accounts is displayed to the customer.
Like the account status information, this information is refreshed once per
20 session.

Other options available to the customer from the account summary screen is the ability to maintain their user profile. This includes maintenance of the e-mail address entered in the sign up process or in a previous maintenance session, changing a password (once the old password is entered), changing challenge questions, adding personal loans to their business online profile or selecting or deleting accounts from their online profile. The selection of accounts is available because the customer may have previously
25

failed the verification of ownership of the account, the account has been originated since the customer signed up for online access, or the account now has web-enabled access.

When adding additional accounts to their online profile, the level
5 of hierarchy previously verified is compared against the highest level of the
accounts selected for addition. If the requested accounts are lower or equal to
the verification level, the accounts are automatically enabled in the customer's
online profile. If the requested accounts are higher than the previously passed
hierarchy level, the verification questions related to the highest of the
10 requested accounts are presented to the customer for completion. In this case,
the requested accounts are not added to the customer's online profile until they
successfully pass the verification of ownership questions.

Although the present invention has been described in relation to
particular embodiments thereof, many other variations and other uses will be
15 apparent to those skilled in the art. It is preferred, therefore, that the present
invention be limited not by the specific disclosure herein, but only by the gist
and scope of the disclosure.